2011-03

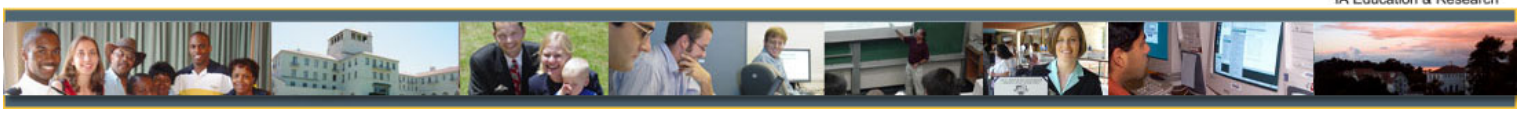
Center for Information Systems Security Studies and Research (CISR) Projects / HASP Program

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Search Site

Centers of Academic Excellence
IA Education & Research



Research: Projects: HASP

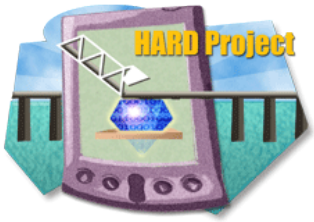
HASP - The High Assurance Security Program
This program provides a unifying conceptual framework and management structure for long range planning and coordination of focused Information Assurance research projects. The primary program goal is to support the strengthening of assurance provided by the National Information Infrastructure. Our approach includes the research and development of high assurance networks, systems, components and tools, and the open dissemination of outputs from those efforts, such as code and documentation.

Open distribution of program outputs provides widespread availability of diamond hard Information Assurance solutions, as well as crystal clear examples and guidance for high assurance solutions developed elsewhere.

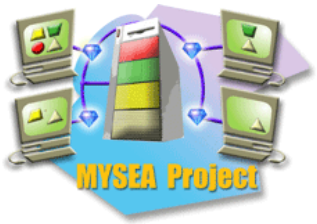
HASP Projects

TCX - Trusted Computing Exemplar Project
The purpose of the Trusted Computing Exemplar project is to provide a working example to show how trusted computing systems and components can be constructed. A prototype *high assurance development framework* will be created first, and then used to produce a reference implementation *trusted computing component*, the *Embedded MicroKernel Prototype*. A third-party *evaluation* of the component will be initiated during development (e.g., once the high-level design documentation is written).

The documentation, source code, development framework and other deliverables will be made *openly available* as they are produced. We will develop a high assurance, embedded micro-kernel and a trusted application built on top of the micro-kernel as a reference implementation exemplar for trusted computing. Because the product as well as the process will be showpieces for trusted computing development, high assurance methodologies and techniques will be applied during the entire lifecycle. The goal is to produce a very small, portable component that will provide users with correct security operation and an *a priori* assurance against system subversion. More...



HARD - The High Assurance Remote authentication Device Project
The HARD project will build and evaluate of a high assurance network access device. The purpose of this device is to provide an unforgeable trusted path with which network clients can securely interact with security-enabled remote servers. HARD will be built upon the Embedded Micro-kernel, developed in the Trusted Computing Exemplar Project (TCX), and will utilize protocols and client/server security mechanisms developed in the MYSEA project. The evaluation portion of this project will encompass the definition of a high assurance Common Criteria protection profile for network access devices, production of the evaluation evidence, as well as support for the government evaluation team in its evaluation activities. More...



MYSEA - Monterey Security Architecture
The purpose of this research project is to develop high assurance security services and integrated operating system mechanisms that will protect distributed multi-domain computing environments from malicious code and other attacks. More...

This page was last modified: March 2011